(19) Europäisches Patentamt
European Patent Office
Office européen des brevets

(11) EP 0 652 540 B1

(12) EUROPEAN PATENT SPECIFICATION

(45) Date of publication and mention of the grant of the patent:
20.09.2000 Bulletin 2000/38

(51) Int. Cl.[7]: **G07F 7/12**

(21) Application number: **94308181.0**

(22) Date of filing: **07.11.1994**

(54) Self-service business system

Selbstbedienungssystem für Schaltergeschäfte

Système libre service pour affaires à guichets

(84) Designated Contracting States:
DE ES FR GB IT

(30) Priority: **08.11.1993 GB 9323489**

(43) Date of publication of application:
10.05.1995 Bulletin 1995/19

(73) Proprietor:
NCR International, Inc.
Dayton, Ohio 45479 (US)

(72) Inventor: **Sime, Iain R. F.**
Dundee, Tayside DD2 1AW, Scotland (GB)

(74) Representative:
Cleary, Fidelma et al
International IP Department
NCR Limited
206 Marylebone Road
London NW1 6LY (GB)

(56) References cited:
GB-A- 2 150 330
GB-A- 2 185 937
GB-A- 2 237 670
US-A- 3 906 460

EP 0 652 540 B1

Printed by Xerox (UK) Business Services
2.16.7 (HRS)/3.6

Description

[0001] The present invention relates to a self-service business system.

[0002] Fraudulent use of self-service business systems such as automated teller machine (ATM) systems has become a substantial problem for banks and other financial institutions. Customer complaints have been received that "phantom withdrawals" have been made from their accounts by persons passing themselves off as the customers.

[0003] In an attempt to reduce the likelihood of fraud occurring, it is known to use biometrics for confirmation of user identity in a self-service system. Biometrics relates to the analysis of biological observations and phenomena. More particularly, in the present context, it relates to the measurement and evaluation of certain physical characteristics which vary from person to person. Biometric identification systems have been developed and are in use today. The publication "Electronic Banking 1", published by "POST-NEWS", Stoke-sub-Hamdon, Somerset TA14 6BR England, discusses the use of biometrics in connection with electronic banking and identifies five types of biometric identification: signature verification, hand geometry, finger and palm print comparison, voiceprint measurement and retinal or iris eye scanning. A sixth type, vein patterns, is identified as having recently been designed. When a biometric assessment is made, a value is calculated for each user. This value is compared with a predefined reference value to decide whether to accept or reject a user. The use of biometrics to confirm the identity of a user is not always completely accurate. Because of the limitations of the technique, there is always a false acceptance rate and a false reject rate. Even though these rates usually lie within the range of 0.1% and 3%, depending upon the biometric used, this can still be unacceptable for banks.

[0004] GB-A-2,237,670 discloses a system for the transfer of value for use in a situation where a user wishes to receive the services or goods from a supplier in return for an appropriate transfer of funds or a commitment to recognize the value of the services/goods supplied. This system comprises a user interface unit having user identification input means, biometric means for producing biometric output data relating to a user, storage means for storing biometric reference data relating to an authorised of the system and is also arranged such that data relating to previous transactions initiated by the authorised user can be stored so that the likely type of transaction to be requested by a given user can be protected having regard to the past request history of that user.

[0005] Accordingly, it is an object of the present invention to provide a self-service system having an improved capability of detecting attempted fraud.

[0006] According to the invention there is provided a self-service system including a user interface unit having user identification means, input means operable by a user for initiating a selected self-service transaction, biometric means for producing biometric output data relating to a user, storage means for storing biometric reference data relating to a plurality of authorised users of the system and arranged to store data relating to previous transactions initiated by said authorised users, prediction means coupled to said identification means and arranged to predict the type of transaction to be requested by a given user on the basis of the stored data relating to previous transactions, transaction authorisation means coupled to said biometric means and to said prediction means and arranged to make a determination as to whether a transaction initiated by a user is to be permitted to proceed to completion, characterized in that said determination is made on the basis that if said biometric output data does not conclusively match said biometric reference data but matches said reference data within a predetermined limit of discrepancy the comparison between the predicted and requested transaction is used in determining whether the transaction is permitted to proceed to completion, and by the system including further storage means arranged to store a suspicion count for each of said authorised users, each suspicion count being arranged to be incremented by one each time said biometric output data for the relevant user is not a conclusive match with said biometric reference data for that user and regardless of the result of the comparison between the predicted and requested transaction, and said transaction authorisation mens being arranged to terminate a transaction if said suspicion count reaches a predetermined threshold value.

[0007] It should be understood that, in a self-service system in accordance with the present invention, if a biometric test is not conclusive, use of the prediction means can be helpful in resolving the identity of the user. The prediction means involves the use of a prediction to determine whether or not a proposed transaction is consistent with the user's normal behaviour in deciding whether to permit the transaction to proceed. A record of past transactions for each user is maintained and stored in a memory in the system. When a user commences a transaction, the system can predict what type of transaction the user is likely to request. In the case in which the biometric evaluation is questionable, the added information with respect to whether the type of transaction selected by the user is consistent with past actions can tip the scales for or against user acceptance.

[0008] Another factor which can be employed in determining whether a requested transaction may proceed to completion is a suspicion count. If a predetermined number of consecutive suspicious transactions involving a particular user have taken place, this can be determinative of user rejection in close cases. A suspicion count for each user is maintained in memory and is incremented for each suspicious transaction. The count

is decremented to a start value (e.g. zero) whenever a non-suspicious transaction involving that user takes place.

[0009] One embodiment of the invention will now be described by way of example with reference to the accompanying drawings, in which:-

Fig. 1 is a block diagram of a self-service system in accordance with the invention incorporating a plurality of ATMs;

Fig. 2 is a schematic diagram of one of the ATMs of Fig. 1; and

Fig. 3 is a flow diagram illustrating the operation of the transaction authorisation means of the system.

[0010] Referring to Figs. 1 and 2, the self-service business system shown therein includes a plurality of ATMs 10 connected in conventional manner to a host computer 12. As shown in Fig. 2, each ATM 10 includes a conventional user interface unit or fascia 14 incorporating key operated input means 16 for enabling a user of the ATM 10 to enter, if required, a personal identification number (PIN) and to select desired services provided by the ATM 10, a lead-through display screen 18 for indicating to the user the options available to him in carrying out a transaction on the ATM 10 and for indicating the keys of the input means 16 which require to be operated in order to select a desired service or services, and a card reader 20 for reading account information contained on an identification card which the user inserts in operation into a slot (not shown) forming part of the card reader 20 whereby the user can be identified. Other conventional modules included in each ATM 10 include a cash dispenser 22 for counting and presenting currency notes to a user, a receipt printer 24 for printing receipts to be presented to a user when a deposit or cash withdrawal is made using the ATM 10 and for printing a mini-statement or balance of account statement when requested by a user, a journal printer 26 for printing a record of transactions carried out by the ATM 10, a depository 28 for receiving envelopes containing cash and/or cheques deposited by a user, environmental data source means 30 for providing data as to the time and date of a transaction together with the location of the ATM 10, processing means 32 for controlling the operations of the various elements of the ATM 10, and a communications module 34 for coupling the ATM 10 to the host computer 12.

[0011] The host computer 12 includes a user reference file 36 which includes records of the types of transactions performed by authorised users in previous uses of the system which includes the various ATMs 10, environmental data relating to these transactions, and biometric reference data for each authorised user.

[0012] Also included in each ATM 10 is a predictive system 38 which is arranged to use the information contained in the user reference file 36 for a particular user to ascertain what service or services have been requested most frequently by that user at particular times, dates and locations in the past, and therefore what service or services are most likely to be requested by that user when he next initiates a transaction by inserting his identification card into the card reader 20 of one of the ATMs 10. The processing means 32 of each ATM 10 acts in dependence on the output of the predictive system 38 to cause the ATM 10 to perform certain operations at certain times and in certain sequences in order to cause the ATM 10 to complete a transaction with greater overall speed, and to simplify the decisions and selections which need to be made by the user, if the service or services actually requested is or are the same as the service, or at least some of the services, which have been predicted. Thus, the processing means 32 causes a particular menu to be displayed on the lead-through display screen 18 following initiation of a transaction by a user and following a prediction that particular services are likely to be requested by the user. For example, a simplified menu could be displayed consisting of only four questions, such as: "Do you require £20?", "Do you require £30?", "Do you require a mini-statement?", and "Do you require some other transaction?". Also, immediately following the initiation of a transaction, the ATM 10 could obtain system authorization for, and count out ready for presenting to the owner, a predicted amount of cash in advance of an anticipated withdrawal request. If, for example, a withdrawal request is predicted to be either £20 or £30, then £20 will be counted out since, if £30 is actually requested, a further $10 can readily be counted and added to the already counted amount.

[0013] Also included in the user interface unit 14 of each ATM 10 is a biometric means 40 which receives one or more biometric inputs from a user who is addressing the ATM 10. As has previously been set forth, the biometric information required may include one or more of several types, such as, for example, signature verification, hand geometry, finger and palm print comparison, voiceprint measurement, retinal or iris eye scanning or vein pattern determination. The particular input apparatus will vary in accordance with the particular biometric employed. For example, for voiceprint measurement, a microphone would customarily be used; for signature verification, a pressure-sensitive writing platform might be employed; for hand geometry, a platform on which the customer's hand is placed and sensed could be used, etc. Output data from the biometric means 40 is compared with the biometric reference data on file in the user reference file 36. As a result of this comparison, a first value is derived representative of the difference between the output data and the reference data. The output data is considered to be a conclusive match with the reference data if the first value is less than a predetermined threshold value.

[0014] Included in storage in a memory unit 42 of the host computer 12 is a suspicion count. This is a count of the number of consecutive suspicious transac-

tions performed by a user. A suspicious transaction is one in which output data from the biometric means 40 fails to match conclusively the reference biometric data for the relevant user but lies within a predetermined limit of discrepancy. Each time that a suspicious transaction takes place, the total of the suspicion count is incremented by one. On the other hand, when a non-suspicious transaction is completed by a user, the suspicion count is decremented to zero. A suspicion count threshold number, either for a particular user or for all users, may be determined and stored in the host computer 12, for example in the user reference file 36.

[0015] Also included in each ATM 10 is a transaction authorisation module 44, which is a software module that is integrated into the processing means 32 which controls the operation of the ATM 10, the module 44 serving to authorise a transaction selected by a user. The inputs to the transaction authorisation module 44 are as follows: the predicted transaction; the actual requested transaction; the biometric value for the user; the biometric reference value; and any previously recorded suspicion count. The outputs from the transaction authorisation module 44 are: OK, meaning that the identity of the user has been confirmed and that the user can proceed with the transaction; failed, meaning that the biometric test has not confirmed the identity of the user as read from his identification card, thereby implying that an attempted fraud is taking place; and suspicious, meaning that the module 44 cannot be 100% sure either way. In the last instance, the suspicion count in the memory unit 42 is incremented by one, so that the system is aware of a possible attempted fraud. It should be understood that if the suspicion count reaches a predetermined threshold value (typically 3) then the module 44 terminates the transaction.

[0016] The operation of the self-service system, particularly as regards the transaction authorisation process, will now be described with reference to Fig. 3. A transaction is initiated (block 50) by a user inserting his identification card into the card reader 20 of one of the ATMs 10. After a transaction is initiated, a biometric check of the user is made (block 52), and simultaneously a prediction is made (block 54) as to the service or services that will probably be requested by the user. At the same time, a suspicion count, if there is one for that user, is forwarded by a path 56 to the transaction authorisation module 44. The user then makes an actual transaction selection (block 58). All of the information from these actions is input to the module 44, as represented by a biometric reference path 60, a biometric value path 62, the suspicion count path 56, a predicted transaction path 64 and an actual transaction path 66. The module 44 then processes all of this information and provides a decision. The various alternatives are represented in Fig. 3 by paths 68, 70 and 72, shown as outputs from the module 44, which lead to blocks 74, 76 and 78, respectively.

[0017] It should be understood that if the biometric value is a conclusive match with the reference value then the transaction continues (block 76) regardless of whether the actual transaction is as predicted.

[0018] Also, if the biometric value clearly fails, then the transaction is found not to be valid by the module 44 regardless of whether the actual transaction is as predicted. In this case the transaction is terminated (block 78) and the suspicion count is incremented. Another option in the case of an invalid transaction is to arrange for the relevant ATM 10 to capture the user's identification card.

[0019] If the biometric value is close to the biometric reference value (i.e. is not a conclusive match but matches the reference value within a predetermined limit of discrepancy) and the actual transaction is as predicted, then the module 44 increments the suspicion count and permits the transaction to proceed to completion provided that the suspicion count has not reached the threshold value. If the biometric value is close to the reference value but the actual transaction is not as predicted, the suspicion count is incremented and appropriate further action is taken (block 74) to handle a suspicious transaction, again provided that the suspicion count has not reached the threshold value. This further action may involve repeating the biometric check, making a different biometric check or requiring the user to enter his PIN on the ATM input means 16. If the further biometric check is conclusive or the entered PIN is correct then the transaction is allowed to proceed. On the other hand, if the further biometric check is not conclusive or the PIN is incorrect then the transaction is terminated.

[0020] In an alternative embodiment of a self-service system in accordance with the invention, instead of storing a user reference file in the host computer 12, a data base containing a record of a user's previous transactions and biometric reference data could be stored in the identification card for that user, this data being read out at the same time as the identification data for the user. Also, the suspicion count for the user could be stored in the identification card.

Claims

1. A self-service system including a user interface unit (14) having user identification means (20), input means (16) operable by a user for initiating a selected self-service transaction, biometric means (40) for producing biometric output data relating to a user, storage means (36) for storing biometric reference data relating to a plurality of authorised users of the system and arranged to store data relating to previous transactions initiated by said authorised users, prediction means (38) coupled to said identification means (20) and arranged to predict the type of transaction to be requested by a given user on the basis of the stored data relating to previous transactions, transaction authorisation

means (44) coupled to said biometric means (40) and to said prediction means (38) and arranged to make a determination as to whether a transaction initiated by a user is to be permitted to proceed to completion, characterized in that said determination is made on the basis that if said biometric output data does not conclusively match said biometric reference data but matches said reference data within a predetermined limit of discrepancy the comparison between the predicted and requested transaction is used in determining whether the transaction is permitted to proceed to completion, and by the system including further storage means (42) arranged to store a suspicion count for each of said authorised users, each suspicion count being arranged to be incremented by one each time said biometric output data for the relevant user is not a conclusive match with said biometric reference data for that user and regardless of the result of the comparison between the predicted and requested transaction, and said transaction authorisation mens (44) being arranged to terminate a transaction if said suspicion count reaches a predetermined threshold value.

2. A system according to Claim 1, characterized in that said transaction authorisation means (44) is arranged to allow a transaction to proceed if said biometric output data conclusively matches said biometric reference data, regardless of the comparison between the predicted and requested transaction.

3. A system according to Claim 2, characterized in that a first value is derived representative of the difference between said biometric output data and said biometric reference data, said output data being considered to be a conclusive match with said reference data if said first value is less than a predetermined threshold value.

4. A system according to either Claim 2 or Claim 3, characterized in that, if said biometric output data does not conclusively match said biometric reference data but does match said reference data within said predetermined limit, and said requested transaction is not consistent with said predicted transaction, said transaction authorisation means (44) is arranged to cause said system to obtain additional information concerning the relevant user before a final determination is made as to whether the transaction is permitted to proceed to completion.

5. A system according to Claim 4, characterized in that in the course of a transaction a further use is made of said biometric means (40) to provide said additional information.

6. A system according to Claim 4, characterized in that in the course of a transaction the user enters a personal identification number by means of said input means (16) to provide said additional information.

7. A system according to any one of the preceding claims, characterized in that said user identification means (20) is formed by a card reader for reading from a card account information relating to a user.

8. A system according to any one of the preceding claims, characterized in that the stored data relating to previous transactions is updated each time a transaction is initiated by one of said authorised users.

9. A system according to any one of the preceding claims, characterized by a host computer (12) and a plurality of automated teller machines (10) each including a user interface unit (14), prediction means (38) and authorisation means (44) as specified in Claim 1.

Patentansprüche

1. Ein Selbstbedienungssystem mit einer Benutzer-Interface-Einheit (14), mit einer Benutzer-Identifizierungs-Einrichtung (20), einer Eingabeeinheit (16), die von einem Benutzer zur Einleitung einer ausgewählten Selbstbedienungstransaktion betätigbar ist, einer biometrischen Einrichtung (40) zur Erzeugung von benutzerbezogenen biometrischen Ausgangsdaten, einer Speichereinrichtung (35) zur Speicherung biometrischer Referenzdaten bezüglich einer Mehrzahl autorisierter Benutzer des Systems und Speicherung von Daten bezüglich früherer Transaktionen, welche von den autorisierten Benutzern eingeleitet wurden, einer mit der Identifizierungseinrichtung (20) gekoppelten Vorhersage-Einrichtung (38) zur Vorhersage der von einem bestimmten Benutzer angeforderten Transaktionsart auf Grundlage gespeicherter Daten über zurückliegende Transaktionen, einer mit der biometrischen Einrichtung (40) und der Vorhersage-Einrichtung (38) gekoppelten Transaktions-Autorisierungseinrichtung (44), welche eine Entscheidung darüber trifft, ob eine von einem Benutzer eingeleitete Transaktion zu Ende geführt werden darf, **dadurch gekennzeichnet**, daß diese Bestimmung auf der Grundlage erfolgt, daß im Falle einer nichtschlüssigen Übereinstimmung der biometrischen Ausgangsdaten mit den biometrischen Referenzdaten, jedoch eine Übereinstimmung mit den Referenzdaten innerhalb einer vorbestimmten Diskrepanzgrenze der Vergleich zwischen der vorhergesagten und der angeforderten Transaktion benutzt wird, um zu bestimmen, ob

die Transaktion fertig durchgeführt werden darf, und daß das System weiterhin eine Speicheranordnung (42) enthält, um für jeden der autorisierten Benutzer einen Verdachtszählwert zu speichern, welcher jedesmal um 1 erhöht wird, wenn die biometrischen Ausgangsdaten des betreffenden Benutzers nicht schlüssig mit den biometrischen Referenzdaten für diesen Benutzer übereinstimmen, und zwar unabhängig vom Ergebnis des Vergleichs zwischen der vorhergesagten und der angeforderten Transaktion, und daß die Transaktions-Autorisierungseinrichtung (44) die Transaktion abbricht, wenn der Verdachtszählwert einen vorbestimmten Schwellwert übersteigt.

2. System nach Anspruch 1, **dadurch gekennzeichnet**, daß die Transaktions-Autorisierungseinrichtung (44) unabhängig vom Vergleich zwischen vorhergesagter und angeforderter Transaktion eine Fortsetzung der Transaktion erlaubt, wenn die biometrischen Ausgangsdaten schlüssig mit den biometrischen Referenzdaten übereinstimmen,

3. System nach Anspruch 2, **dadurch gekennzeichnet**, daß ein erster Wert abgeleitet wird, der die Differenz zwischen den biometrischen Ausgangsdaten und den biometrischen Referenzdaten darstellt, und daß die Ausgangsdaten als schlüssig übereinstimmend mit den Referenzdaten angesehen werden, wenn der erste Wert kleiner als ein vorbestimmter Schwellwert ist.

4. System nach Anspruch 2 oder 3, **dadurch gekennzeichnet**, daß dann, wenn die biometrischen Ausgangsdaten nicht schlüssig mit den biometrischen Referenzdaten übereinstimmen, jedoch eine Übereinstimmung mit den Referenzdaten innerhalb einer vorbestimmten Grenze vorliegt, und wenn die angeforderte Transaktion nicht konsistent mit der vorhergesagten Transaktion ist, die Transaktions-Autorisierungseinrichtung (44) derart ausgebildet ist, daß sie dem System eine zusätzliche Information bezüglich des betreffenden Benutzers zukommen läßt, ehe eine endgültige Entscheidung darüber getroffen wird, ob die Fortsetzung der Transaktion erlaubt wird.

5. System nach Anspruch 4, **dadurch gekennzeichnet**, daß im Verlauf einer Transaktion die biometrische Einrichtung (40) zur Lieferung zusätzlicher Information dient.

6. System nach Anspruch 4, **dadurch gekennzeichnet**, daß im Verlauf einer Transkation der Benutzer über die Eingabeeinrichtung (16) eine persönliche Identifikationsnummer zur Lieferung der zusätzlichen Information eingibt.

7. System nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet**, daß die Benutzer-Identifizierungseinrichtung (20) durch einen Kartenleser gebildet wird, der von einer Karte eine benutzerbezogene Kontoinformation abliest.

8. System nach einem der vorstehenden Ansprüche, **dadurch gekennzeichnet**, daß die gespeicherten Daten bezüglich zurückliegender Transaktionen jedesmal aktualisiert werden, wenn eine Transaktion von einem der autorisierten Benutzer eingeleitet wird.

9. System nach einem der vorstehenden Ansprüche, **gekennzeichnet durch** einen Host-Computer (12) und eine Mehrzahl von Bankautomaten (10), deren jeder eine Benutzer-Interface-Einheit (14), eine Vorhersage-Einrichtung (38) und eine Autorisierungseinrichtung (44) gemäß Anspruch 1 enthält.

Revendications

1. Un système libre-service comportant une unité interface utilisateur (14) ayant un moyen d'identification utilisateur (20), un moyen d'entrée (16) opérable par un utilisateur pour déclencher une transaction libre-service sélectionnée, un moyen biométrique (40) pour produire des données de sortie biométriques relatives à un utilisateur, un moyen de mémorisation (36) pour mémoriser des données de référence biométriques relatives à une pluralité d'utilisateurs autorisés du système et arrangé pour mémoriser des données relatives à des transactions antérieures déclenchées par lesdits utilisateurs autorisés, un moyen de prédiction (38) accouplé audit moyen d'identification (20) et arrangé pour prédire le type de transaction susceptible d'être demandé par un utilisateur donné sur les bases des données mémorisées relatives à des transactions antérieures, un moyen d'autorisation des transactions (44) accouplé audit moyen biométrique (40) et audit moyen de prédiction (38) et arrangé pour déterminer si l'on doit permettre à une transaction déclenchée par un utilisateur d'être menée à bien, caractérisé en ce que ladite détermination est faite en partant du principe que si lesdites données de sortie biométriques ne correspondent pas de façon concluante auxdites données de référence biométriques mais correspondent auxdites données de référence dans une limite d'écart prédéterminée, la comparaison entre la transaction prédite et la transaction demandée est utilisée pour déterminer si l'on permet à la transaction d'être menée à bien, et par le système comportant un autre moyen de mémorisation (42) arrangé pour mémoriser un compte des transactions suspectes pour chacun desdits utilisateurs autorisés, chaque compte des transactions suspec-

tes étant arrangé pour être incrémenté d'un à chaque fois que lesdites données de sortie biométriques pour l'utilisateur approprié ne sont pas une correspondance concluante avec lesdites données de référence biométriques pour cet utilisateur et quel que soit le résultat de la comparaison entre la transaction prédite et la transaction demandée, et ledit moyen d'autorisation des transactions (44) étant arrangé pour mettre fin à une transaction si ledit compte des transactions suspectes atteint une valeur de seuil prédéterminée

2. Un système conformément à la revendication 1, caractérisé en ce que ledit moyen d'autorisation des transactions (44) est arrangé pour permettre à une transaction de se poursuivre si lesdites données de sortie biométriques correpondent de façon concluante avec lesdites données de référence biométriques, quelle que soit la comparaison entre la transaction prédite et la transaction demandée.

3. Un système conformément à la revendication 2, caractérisé en ce qu'une première valeur est dérivée, représentative de la différence entre lesdites données de sortie biométriques et lesdites données de référence biométriques, lesdites données de sortie étant considérées être une correspondance concluante avec lesdites données de référence si ladite première valeur est inférieure à une valeur de seuil prédéterminée.

4. Un système conformément à la revendication 2 ou à la revendication 3, caractérisé en ce que, si lesdites données de sorties biométriques ne correspondent pas de façon concluante avec lesdites données de référence biométriques mais correspondent avec lesdites données de référence dans ladite limite prédéterminée, et que ladite transaction demandée n'est pas en accord avec ladite transaction prédite, ledit moyen d'autorisation des transactions (44) est arrangé pour faire en sorte que ledit système obtienne des informations supplémentaires concernant l'utilisateur approprié avant qu'il ne soit déterminé définitivement si l'on permet à la transaction d'être menée à bien.

5. Un système conformément à la revendication 4, caractérisé en ce que, au cours d'une transaction, une autre utilisation est faite dudit moyen biométrique (40) pour fournir lesdites informations supplémentaires.

6. Un système conformément à la revendication 4, caractérisé en ce que, au cours d'une transaction, l'utilisateur entre un code personnel au moyen dudit moyen d'entrée (16) pour fournir lesdites informations supplémentaires.

7. Un système conformément à l'une quelconque des revendications précédentes, caractérisé en ce que ledit moyen d'identification utilisateur (20) est formé par un lecteur de canes pour lire, à partir d'une carte, des informations relatives au compte d'un utilisateur.

8. Un système conformément à l'une quelconque des revendications précédentes, caractérisé en ce que les données mémorisées relatives à des transactions antérieures sont mises à jour à chaque fois qu'une transaction est déclenchée par l'un desdits utilisateurs autorisés.

9. Un système conformément à l'une quelconque des revendications précédentes, caractérisé par un ordinateur central (12) et une pluralité de guichets automatiques bancaires (10), chacun comportant une unité interface utilisateur (14), un moyen de prédiction (38) et un moyen d'autorisation (44) comme spécifié dans la revendication 1.

FIG. 1

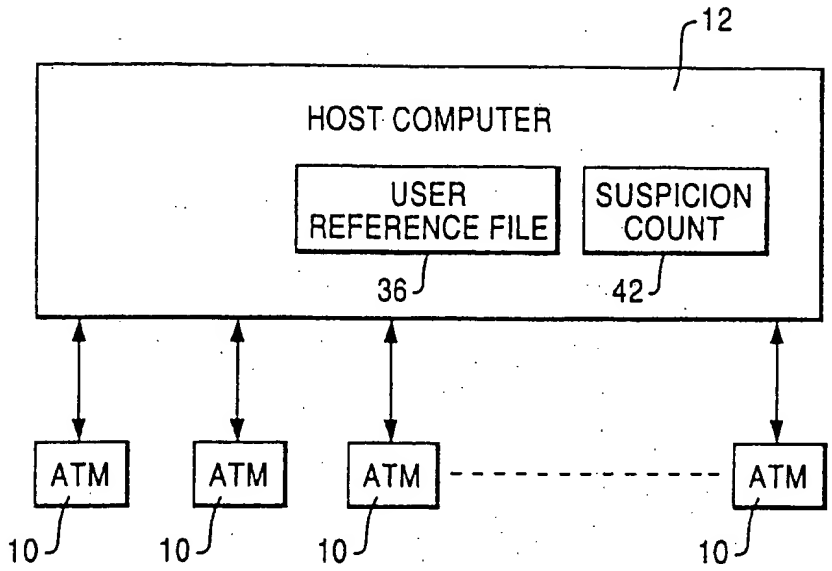
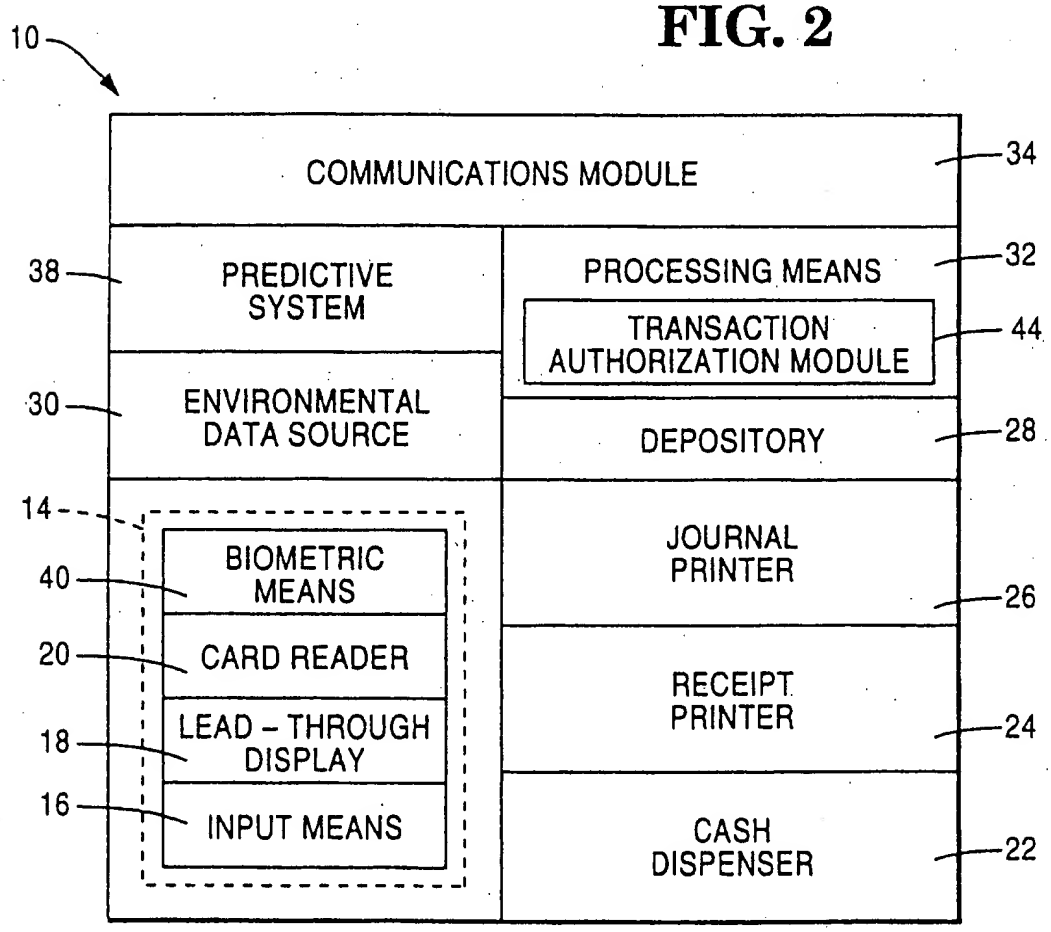

12
HOST COMPUTER
USER REFERENCE FILE
SUSPICION COUNT
36
42
ATM
ATM
ATM
ATM
10
10
10
10

FIG. 2


10
COMMUNICATIONS MODULE
34
38
PREDICTIVE SYSTEM
PROCESSING MEANS
32
TRANSACTION AUTHORIZATION MODULE
44
30
ENVIRONMENTAL DATA SOURCE
DEPOSITORY
28
14
BIOMETRIC MEANS
40
JOURNAL PRINTER
26
20
CARD READER
RECEIPT PRINTER
24
18
LEAD – THROUGH DISPLAY
16
INPUT MEANS
CASH DISPENSER
22

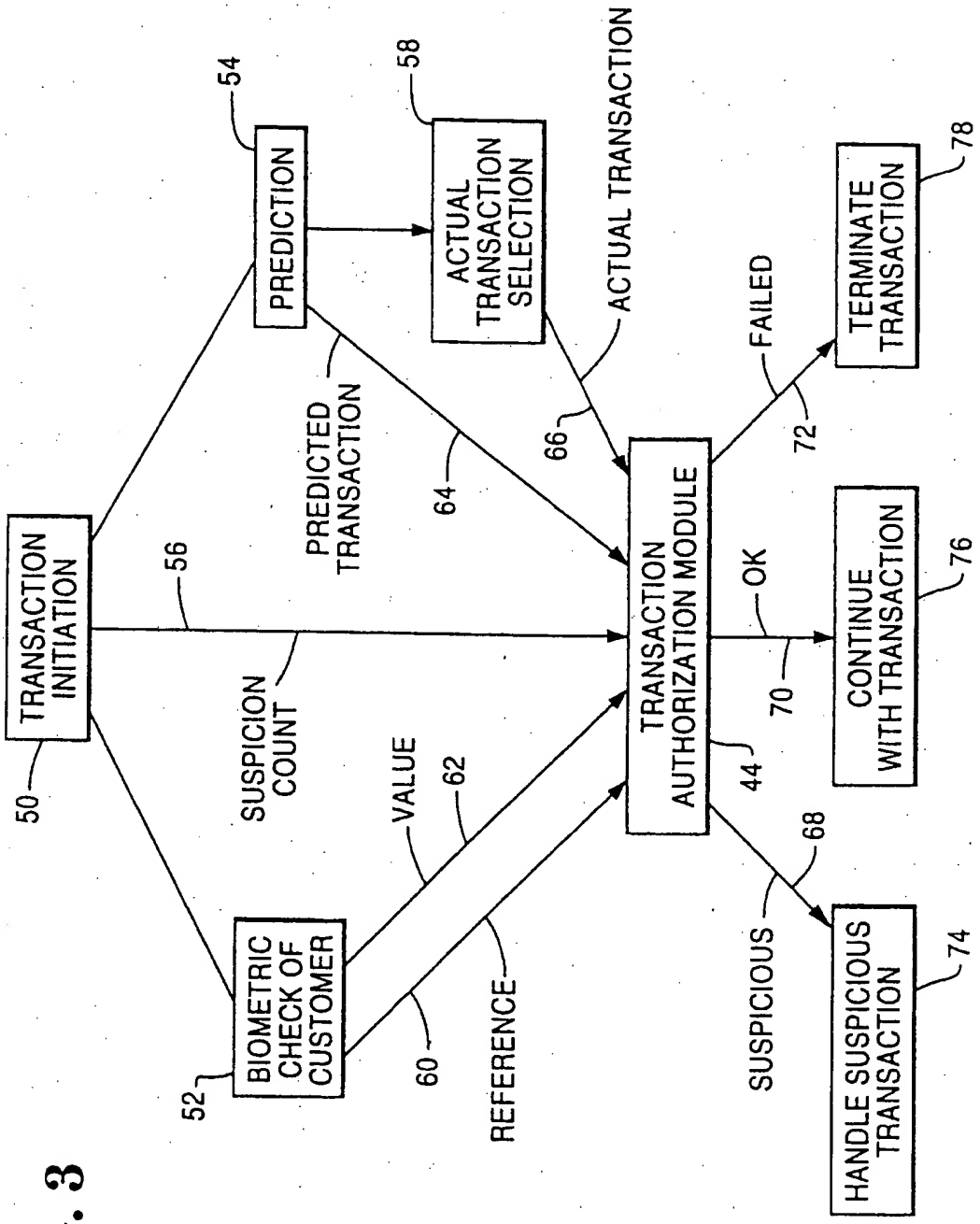

TRANSACTION INITIATION
50
PREDICTION
54
ACTUAL TRANSACTION SELECTION
58
BIOMETRIC CHECK OF CUSTOMER
52
TRANSACTION AUTHORIZATION MODULE
44
TERMINATE TRANSACTION
78
CONTINUE WITH TRANSACTION
76
HANDLE SUSPICIOUS TRANSACTION
74
56
SUSPICION COUNT
PREDICTED TRANSACTION
64
ACTUAL TRANSACTION
66
VALUE
62
REFERENCE
60
FAILED
72
OK
70
SUSPICIOUS
68

FIG. 3